ENC 3

KPMG LLP
Suite 2000
355 South Grand Avenue
Los Angeles, CA 90071-1568

August 25, 2010

The Board of Water and Power Commissioners
Los Angeles Department of Water and Power
Los Angeles, California

Ladies and Gentlemen:

We have audited the financial statements of the Water Revenue Fund (Water System) and the Power Revenue Fund (Power System), enterprise funds of the City of Los Angeles, California for the year ended June 30, 2009, and have issued our report thereon dated November 9, 2009 for the Water System and November 17, 2009 for the Power System. In planning and performing our audit of the financial statements of the Water and Power Systems, collectively referred to herein as the Department, in accordance with auditing standards generally accepted in the United States of America, we considered the Department's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control.

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized in the following pages.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Department's organization gained during our work to make comments and suggestions that we hope will be useful to you.

Managements responses to the control deficiencies identified in our audit are described in the accompanying summary. We did not audit the Department's responses and, accordingly, we express no opinion on the responses.

We would be pleased to discuss these comments and recommendations with you at any time.

This communication is intended solely for the information and use of management, the Board of Water and Power Commissioners, and others within the organization, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

MGT. LTR.
9/16/10

KPMG LLP is a Delaware limited liability partnership, the U.S. member firm of KPMG International Cooperative ("KPMG International"), a Swiss entity.

(1) Inappropriate Access to Migrate Changes to Production

Observation

Based on our testwork over mainframe application program changes, we noted 8 individuals with inappropriate access. These users belonged to the Technical Service Group and did not require access to migrate changes to the production environment as part of their job responsibilities.

Based on our testwork, over PeopleSoft HRMS application program changes, we noted that PeopleSoft HRMS programmers are not restricted from migrating changes to production. Additionally, we noted that programmers also have Security Administrator access.

Effect (or Potential Effect)

Unauthorized changes or transactions may be posted without accountability.

Recommendation

General change control principles suggest that application programmers should not have access to program source or object modules during the approval process. Application programmers should not have update access to programs after they have been approved and before they are moved into production.

To comply with basic general control principles, we recommend the following:

- All changes should be reviewed by a programmer other than the one developing the code to ensure that information will be consistently processed in a controlled environment.
- Changes should be migrated into production by someone other than the developer.
- All approvals (i.e. testing, user acceptance, migration, etc.) should be captured on the Change Request Form.

In addition, we recommend that management enable system logging within the key financial applications. All source code migrated to production by a programmer should be logged and periodically reviewed to ensure that all changes made by a programmer/developer were authorized and appropriately approved. This periodic review of migrated code would help mitigate the risk of potential fraudulent and undetectable modifications to the system and data from occurring.

Management Responses

Mainframe Applications: Effective August 20, 2009, inappropriate users with access to migrate source code into production has been removed. Control auditing has been activated for key libraries.

PeopleSoft HRMS: No plans in changing the security access rights for individuals responsible for administering PeopleSoft HRMS.

However, the Department will be investigating a manual control that will allow auditability of changes through LADWP's Change Management system and a Change Control on the servers.

(Continued)

(2) Informal Process for Application Changes to Mainframe Applications and PeopleSoft HRMS

Observation

During our testwork over PeopleSoft HRMS and Mainframe applications, we noted that no formal documentation of testing completion or programming manager approval exists for modifications.

Effect (or Potential Effect)

The lack of documentation or other formalization of testing completion and approval increases the risk of system instability, downtime, and potential misstatement of figures based on information provided by the application.

Recommendation

We recommend that management consider including in the program change policy, a requirement to retain evidence of program change testing and approvals. Periodic reviews should be performed to ensure compliance with the program change policy.

Management Response

The Department will be verifying that the ITIL Change Management process is being followed.

(3) Inappropriate Access to Network Operations Control Room (Data Center)

Observation

Based on our testwork over physical access to the server room, we identified 49 out of 84 employees with inappropriate access. These 49 employees consist of programmers, locksmiths, electrical repairmen, and other individuals that do not require access to the data center as part of the [illegible] esponsibilities. The 49 exceptions were a result of the restructuring/reorganization of the data center a[illegible]ver room.

Effect (or Potential Effect)

Inappropriate individuals may access the data center and misappropriate LADWP IT Assets.

Recommendation

We recommend that management review the system generated listing of users with access to the Data Center to ensure that only appropriate personnel, with the daily job responsibilities that require access, continue to have access to the Data Center.

On an ongoing basis, we recommend that management develop and implement a formal procedure over the granting and removing of access to the Data Center. Specifically:

- A formal User Request Form should be completed, with approvals, for all data center access requests.
- The confirmation of the user being granted access should be evidenced.

The request and approval evidence should be documented and formally evidenced. A process that evidences the proper approvals required by management will ensure that all users with access are approved and authorized to have direct access to the server room where the financial applications are maintained.

Management Response

Effective August 10, 2009, all users identified as having "inappropriate" access to the data center have been removed. The Department will be implementing a quarterly review process that will incorporate a sign-off procedure to ensure that policy requirements are being met.

(4) Inappropriate Privileged/Super User Access

Observation

Based on our testwork over privileged/super user access to EIS, we noted 1 inappropriate user with administrative, or "VIP", access to the system. This user does not require VIP access to EIS as part of his job responsibility.

Based on our testwork over privileged access on the Windows Domain (Network), we noted 2 inappropriate users with 'Domain Admin' access to the Joint LADWP domains. Only the 'Joint' domain supports financial related key spreadsheets.

Based on our testwork over privileged/super user access to FileNet AP, we noted 16 terminated users with active user IDs to create new users, modify existing users, and modify access roles within FileNet AP. Subsequent to our review, these user IDs were deleted from FileNet AP.

Based on our testwork over privileged access/super user access within the IPRS system, we noted 5 out of 8 users with inappropriate access. These users do not require 'Connect' authority, which grants the ability to connect RACF IDs to the IPRS system, as part of their job responsibilities.

Effect (or Potential Effect)

Unauthorized changes or transactions may be posted without accountability.

Recommendation

We recommend that management consider performing periodic access reviews over employees with administrative access to key financial applications.

Management Responses

EIS: Effective August 6, 2009, Derrick Snearl's VIP access was revoked.

Network: Effective August 20, 2009, inappropriate Domain Admin access to the Joint Domain was removed. The Department will be implementing a quarterly review process that will incorporate a sign-off procedure to ensure that policy requirements are being met.

IPRS: The Department will be implementing a quarterly review process that will incorporate a sign-off procedure to ensure that policy requirements are being met.

(5) Shared IDs

Observation

Based on our testwork over super user access to the Bottomline Checkwriting application, we noted that the Bottomline Checkwriting admin account, "Supervisor", is a shared account. The password to the

Supervisor account was last changed on December 8, 2006. The number of users that know the password is unknown.

Based on the security limitations of RCAS, the account "RCA" is a single administrator account that cannot be assigned to individual users, thus the password to this account is shared between 2 RCAS administrators. Individuals with access to this account are able to add, modify, and disable any RCAS user accounts. Additionally, the password to the shared account had not been changed during the period under review and the date when the password was last changed is unknown.

Effect (or Potential Effect)

Unauthorized changes or transactions may be posted without accountability. The shared nature of user accounts compromises individual accountability as there is no way to identify or trace the specific individuals who have used it.

Recommendation

Authorized administrators should be administering the system with unique individual user IDs rather than generic system accounts/shared accounts. We recommend that, where possible, all accounts have an owner associated with them and each user only have one account. As noted above, this includes documenting the controls in place to ensure that appropriate users access the vendor or system IDs. If the system does not allow for administrative privileged to be uniquely assigned to individuals, we recommend the passwords be changed on a regular basis and documentation retained to evidence the periodic change of the shared passwords.

Management Responses

Bottomline Checkwriting: No action taken. Bottomline's/Paybase SUPERVISOR account comes default with the package software. It is only used to install, upgrade, and configure the Paybase package software; it does not have designer/development access nor access to printing checks. Separation of duties is built-in.

RCAS: The Department is in the process of finalizing an RACF-based security control on all of the RCAS transactions, enabling us to manage access from RACF.

The Department will be implementing a quarterly review process that will incorporate a sign-off procedure to ensure that policy requirements are being met.

(6) Password Parameters

Observation

Based on our testwork, we noted that the domain policy over password parameters is not configured in accordance with the 'Los Angeles Department of Water and Power Information Security Policy'. The Policy states that the minimum length should be 8 alphanumeric characters; however, the domain is configured with 7 characters, and the complexity configuration is disabled.

Effect (or Potential Effect)

Increases the risk of unauthorized access to the network by external or internal parties.

Recommendation

We recommend that management implement the password requirements as noted in the 'Los Angeles Department of Water and Power Information Security Policy'.

Management Response

Bulletin issued in August 2009 indicating minimum password length should match the stated policy. Changes to make Active Directory congruent with Information Security Policy have been completed.

(7) Configuration of Access Rules

Observation

No special authorization is required to access MCS, once a user has obtained a valid RACF mainframe user account. This is a system limitation and the MCS application does not have the capability to enforce role-based security. Access to MCS is not restricted further, there is no additional level of authorization required to access MCS. Any user with a RACF mainframe user account (with the proper knowledge of commands) can update data in MCS.

RACF security is configured to assign a user a specific menu/transaction path to allow them access to an application. Not all users are granted the same RACF privileges. If a user is assigned the menu/transaction to allow them to access MCS, there are no further restrictions at the application level.

Effect (or Potential Effect)

Unauthorized inventory transactions may be posted without accountability.

Recommendation

We recommend that management assess the security configuration of the MCS application and consider restricting access to MCS transactions to individuals based on job responsibility.

Management Response

Effective August 31, 2009, to comply with the finding regarding IMS transaction security, additional security provisions were enabled on the Material Control System (MCS) and Integrated Purchasing and Receiving System (IPRS). Effective Monday, August 31, 2009, at noon, IMS transaction security was enabled at which time any employee, who had not been authorized, was no longer able to run any MCS and IPRS transactions.

(8) Periodic Review of User Access Rights

Observation

Based on our testwork, we noted that no periodic review of network user access exists, nor does any periodic review of user access and roles/segregation of duties within several specific in-scope applications (Walker GL, RCAS, MCS, EIS, PeopleSoft HRMS, Filenet AP, Bottomline Checkwriting).

Effect (or Potential Effects)

Increases the risk of unauthorized access to in-scope applications.

Recommendation

We recommend that management should implement processes and procedures for conducting user access reviews. These reviews should be performed in collaboration with business units and the IT department since the business unit has knowledge on the processes and business rules of their department. Evidence of such reviews should be logged and kept. A detailed review should be performed over the validity of all users and their access to the critical systems. This review should be conducted to ensure that only active employees have access to the network, and appropriate users have access to the critical systems and their access is aligned with their job responsibilities. Based on the results of the review, management should undertake appropriate steps to make necessary adjustments to user access to the critical systems.

We recommend that management create a role-based security access matrix, which should list, at a minimum, the transactions that should not be grouped together and profiles that should not be assigned together that would result in a segregation of duties conflict. Careful consideration should be taken into account for roles or profiles that are determined to be a conflict to ensure that a segregation of conflict is maintained. This matrix should be reviewed during the maintenance/creation of profiles and during the assignment of user access.

In addition, users' access should be reviewed against the access matrix to ensure that user access is in compliance with the Department's segregation of duty polices. Compensating controls will be required in situations where users may have segregation of duty conflicts, but are required to have the access to perform their jobs. Based on the results of the review, management should undertake appropriate steps to make necessary adjustments to user access to the critical systems.

Management Response

The Department will be implementing a quarterly review process that will incorporate a sign-off procedure to ensure that policy requirements are being met.

(9) Access Provisioning

Observation

During our test of operating effectiveness over ne[illegible]s added to the EIS system, we noted that documented evidence for approval for 4 out of 8 sampled did not exist.

Effect (or Potential Effect)

Increases the risk of unauthorized access to the EIS system.

Recommendation

We recommend that management reiterate the policy requiring approval of access by a requestor's supervisor prior to granting a user access to the system. Additionally, evidence of approval should be retained for a minimum period of 13 months.

Management Response

As of September 1, 2009, EIS has been secured by RACF security enabling us to manage access from RACF. We will be implementing a quarterly review process that will incorporate a sign-off procedure to ensure that policy requirements are being met.

(10) Backup and Recovery Process

Observation

Based on our testwork over backup and recovery procedures, we noted that testing over the restoration of data is performed; however, evidence over the restoration testing is not retained. Moreover, the testing does not include procedures that validate the completeness and accuracy of the restored data.

Effect (or Potential Effect)

Without properly testing the recoverability of data backups, the integrity of the data backed up is unknown and may be unusable in the event data restoration is required.

Recommendation

We recommend that management consider implementing periodic data restoration testing, which includes end-user testing/validation. Results of the data restoration testing should be documented and retained.

Management Response

The Department will be implementing a regular review process that will incorporate a sign-off procedure to ensure that tested backups are validated.

(11) Access to update/modify employee master data in PeopleSoft HRMS

Observation

During our testwork over user access to update/modify employee master data within PeopleSoft HRMS, we noted that 6 out of 15 users have inappropriate access. These 6 users do not have a valid business need for such access. The 6 inappropriate users comprise of 1 PeopleSoft Security Administrator and 5 programmers.

Effect (or Potential Effect)

Unauthorized employee payroll changes or transactions may be posted without accountability.

Recommendation

We recommend that management consider monitoring the activities of PeopleSoft HRMS privileged users to help ensure no unauthorized updates are performed.

Management Response

Changes made in HRMS do not affect or influence EIS or the payment of employees as it is not the authoritative source for payroll generation. Additionally, we will be verifying that the ITIL Change Management process is being followed for provisioning access. Additionally, we will be implementing a quarterly review process that will incorporate a sign-off procedure to ensure that policy requirements for access are being met. We will also be deploying a solution that will allow auditing of application access, from a network layer, with the deployment of a product called Packet Sentry.

(12) Vacation Liability

Observation

During our test of operating effectiveness, we noted that the formula for the computation of the Vacation Liability Amount for each employee is calculating the employees' Vacation Balance (in hour:minute form) as a whole number instead of an hour-minute number. In other words, the formula is treating the minute balance of an employee's vacation hours as a fraction of 100 minutes rather than as a fraction of 60 minutes.

Effect (or Potential Effect)

Potential understatement of the Vacation Liability Amount for each employee with a minute balance other than "0".

Recommendation

We recommend that management assess the EIS configuration over computing the vacation liability amount and modify it accordingly to help ensure a more accurate calculation.

Management Response

LADWP's Payroll Department is aware of the calculation in the Vacation Liability Report used for the accrual of the Vacation Liability. The figure given by the calculation provides an estimate, not an actual amount paid to employees upon retirement. It is management's position that this issue is immaterial to the overall financial statements.

(13) Access to Receive Inventory in IPRS

Observation

During our testwork, we noted 24 out of 330 users with inappropriate Type 1 access to receive inventory in IPRS. These individuals did not require this level of access to perform their job function.

Effect (or Potential Effect)

Unauthorized inventory receiving transactions may be posted.

Recommendation

We recommend that management assess the appropriateness of users with access to receive inventory in IPRS and remove those users identified as not having a business need. Additionally, periodic access reviews should be performed.

Management Response

As of September 1, 2009, IPRS transactions have been RACF-secured [through the Resource Access Control Facility (RACF) mainframe security system used to control access to mainframe-based applications], enabling the Department to manage access from RACF. The Department will be implementing a quarterly review process that will incorporate a sign-off procedure to ensure that policy requirements are being met.

(14) Financial Reporting Review of Statement of Cash Flows

Observation

During our initial review of the statement of cash flows (Water System) under the direct method, we identified that management had included $181,530,000 in cash receipts from customers when the amount should have been included in cash receipts from customers for other Agency services.

Similarly, during our initial review of the statement of cash flows (Power System) under the direct method, we identified that management had included $127,800,000 in cash receipts from customers when the amount should have been included in cash receipts from customers for other Agency services.

Effect (or Potential Effect)

The lack of effective controls in place over the preparation of financial statements and related disclosures may lead to the Power and Water Systems producing financial information that does not adhere to U.S. GAAP.

Recommendation

Management should evaluate the design and effectiveness of financial reporting controls currently in place to ascertain that all significant reporting matters are addressed in the Department's financial statements every reporting period prior to third-party distribution.

Management Response

The review of the financial statements was done concurrently between KPMG and management. Had management completed their review prior to KPMG's review, the error would have been identified. Management has a system generated report that includes the funds collected from customers on behalf of other agencies, which is used by management for this purpose. Additionally, the information reported and presented in the cash flow in fiscal years 2007 and 2008 was correct. Therefore, management believes to have the tools and the ability to identify reporting errors like the one described above had management's review occurred prior to KPMG's review rather than concurrently. Thus, it appears that the correction is an oversight and not indicative of a deficiency in management's review process.

(15) Incorrect Presentation of Completed Projects as "Construction Work In Progress (CWIP)"

Observation

To test the accuracy and completeness of completed project transfers from CWIP to utility plant for the Water System, we obtained supporting documentation from project managers and engineers that indicated whether the project was completed or still in process. For five of the eight transfers tested, the accounting department was not timely notified of the completion of those projects.

Effect (or Potential Effect)

Depreciation expense may be understated if projects are not transferred to Utility Plant upon their completion. Based on the results of our procedures, we extrapolated the impact of these errors to be an understatement of $18 million in depreciation expense.

Recommendation

Management should have timely communications between the engineers and the accounting staff. This will enable the accounting department to perform a more thorough review of completed construction projects so that completed projects are transferred to Utility Plant and start depreciating in a timely manner.

Management Responses

During fiscal year 2009, the Water System implemented a Project Reporter System so that the progress on capital projects could be monitored more efficiently. The accounting department used the data in this system to reclassify work orders from CWIP to utility plant instead of waiting for the notification via email. From the testing of the control, different dates were reported as to the completion date verbally given versus what was reported in the new system.

The Department is comfortable that the difference between the Project Reporter System and manual email process is inconsequential. The difference between the dates in question is a matter of a few months in each instance. The Department has a financial planning system that monitors deprecation at a company level so if the difference was more than inconsequential it would be brought to management's attention via our monthly performance reports.

In addition to the system, the manager of the work order classification group has access to the budget system to determine any other information to support the status of the project and RCAS. The work order classification group sends inquiries to project managers when the data they are seeing in RCAS/Budget/or Project Reporter is not clear on what is happening with the project. These steps, along with working with the project managers and budget coordinators as necessary, are steps that we have taken to ensure the amounts in CWIP are correct.

(16) Allowance for Doubtful Accounts Methodology

Observation

The Department's methodology to calculate the allowance for doubtful accounts is based on historical bad debt write-off as a percentage of revenue. CIS is programmed to write off inactive or closed accounts that are over 120 days old. However, for customers who receive a statement bill with multiple accounts (e.g. City of LA Harbor), if they default payment on any single account on the statement, they are still considered active in the CIS system; therefore, old balances for these statement customers never get written off or be factored into the allowance calculation. This may lead to overstatement of accounts receivable.

Review of the CIS accounts receivable aging report is a potential mitigating control; however, the CIS system is unable to further disaggregate the "over 90 days" aging bucket due to system limitations.

Effect (or Potential Effect)

To calculate the Department's allowance for doubtful accounts, the Department needs to rely on a report that can accurately identify delinquent accounts. System limitations over the identification of inactive or closed customer accounts over 120 days old complicates this process. The lack of accurate information may result in an overstatement of the accounts receivable balance.

Recommendation

The Department should determine if the above system limitations can be overcome and evaluate the design and effectiveness of the manual controls currently in place to ascertain the accuracy and completeness of the Department's allowance for doubtful accounts.

Management Response

The Department is in the process of replacing the current billing system and will work with the new system implementer to design a more usable accounts receivable aging report. The new system should be in place in 2012. Until the system is available, management will utilize the information available to determine an appropriate allowance for doubtful accounts as not to overstate the Department's receivables.

(17) Entity Level Controls

Observation

One of the Department's policies requires all new employees to sign a statement that they have read and understood the City's Code of Ethics Policy. However, the Department was not able to find one of the fifteen samples we selected for testing.

The Department also has a policy to perform resume and background checks on employees to ensure they have the adequate knowledge to perform their job requirements. However, the Department was not able to find one of the fifteen samples we selected for testing.

Effect (or Potential Effect)

The deficiencies in the above entity level controls were not determined to have a material impact on the financial statements. However, they do represent a breakdown in the Department's entity level control policies.

Recommendation

Management should periodically monitor all entity level controls to ensure they are operating as designed and that corrective action, if necessary, is taken on a timely basis.

Management Responses

The Department has obtained a signed ethics statement from the one employee who was found not to have previously signed one and has recommunicated to Personnel staff that this is a required form.

In addition, the Department has completed a background check for the one employee in question. All employees are required to be finger printed and have a background check completed on them. Procedures have been updated to ensure that all civil service and exempt employees hired from the Union Hall complete a civil service application so that any criminal history is disclosed and appropriately documented.

(18) Incorrect recording of cost incurred to remove fixed assets

Observation

During testing of accumulated depreciation, we noted that the Department was reducing accumulated depreciation to account for cost incurred to remove fixed assets, but that the depreciation rate did not have a sufficient component to capture the cost of removal. This resulted in an understatement of accumulated depreciation and operating expenses of $0.4M and $18.9M for Water and Power System, respectively.

Management was recording the removal costs as an offset to accumulated depreciation because they believed that their depreciation rates had factored in the costs to remove an asset when it is retired. For the 2009 financial statement audit, cost of removal and salvage value were considered offsetting requiring no additional expense to be recorded. However, upon inspection of the depreciation study used in the testing of depreciation and amortization expenses, we verified that management excludes the cost of removal in the depreciation rates for most of its fixed assets. As a result, management should not be decreasing accumulated depreciation when it incurs costs to remove these assets as these costs were not factored into the depreciation rate. The amount should be recorded as other operating expenses.

Effect (or Potential Effect)

We proposed an audit difference of $18.9M for the Power Fund as a result of this deficiency. Based on the amount of these transactions in the current year, management believes the likelihood and magnitude of this deficiency causing a material misstatement to be remote and inconsequential, respectively.

Recommendation

Management should have a control in place to perform periodic reviews of retired fixed assets to ensure that the removal costs is not recorded as an offset to accumulated depreciation.

Management Response

Effective January 1, 2010, management updated the depreciation rates for distribution assets to recover the cost of removal over the lives of the assets. The rate used is from a formal Depreciation Study conducted by Deliotte & Touche LLP in 2004. Management believes that the increase in rate will more accurately fully recover the cost of removal expense over the life of the asset.